Title: SYSTEM AND METHOD UTILIZING CLEAN GROUPS FOR SECURITY MANAGEMENT
Inventors: A. Shelest et al.
Docket No.: MSFT121932

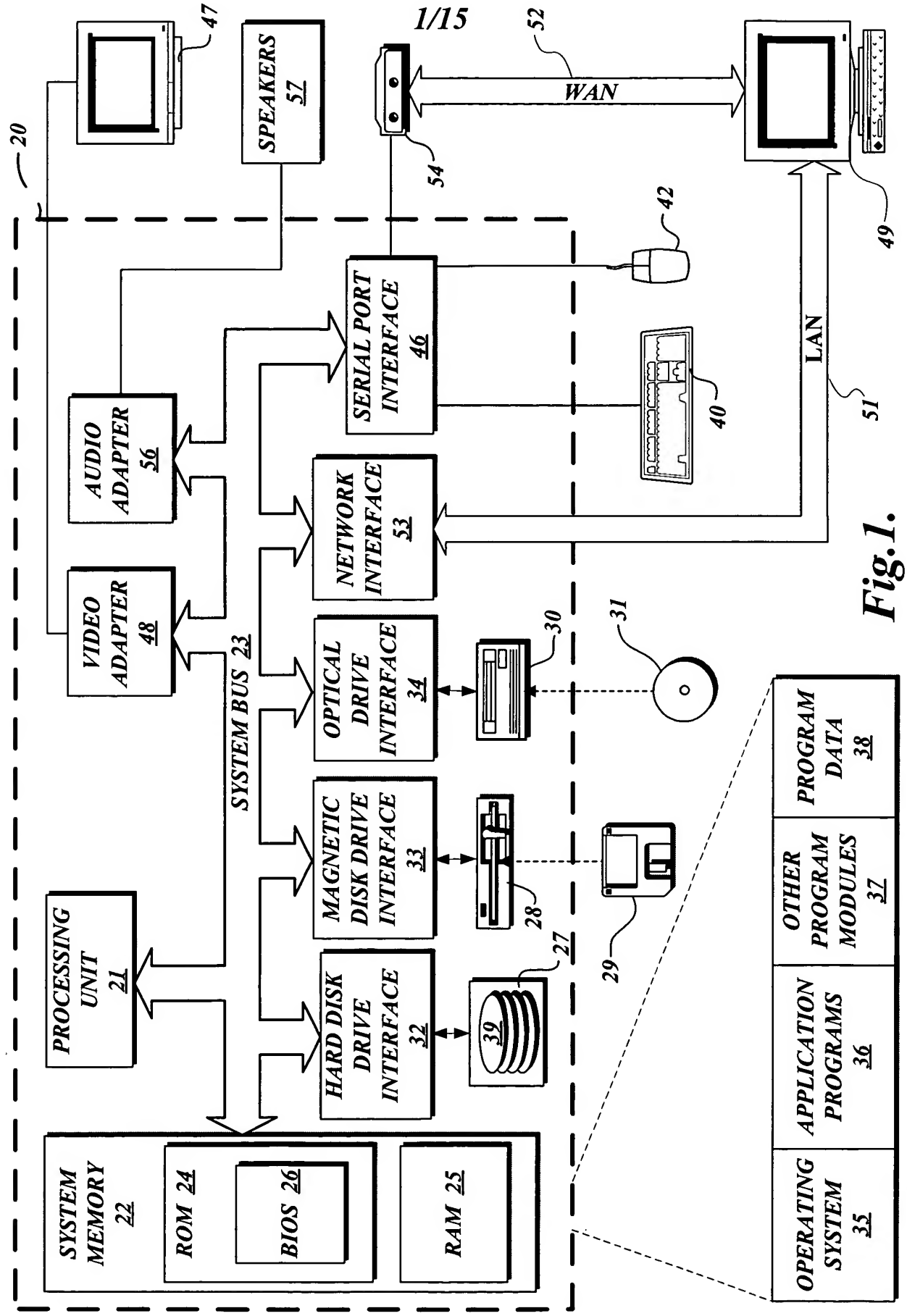

Fig. 1.

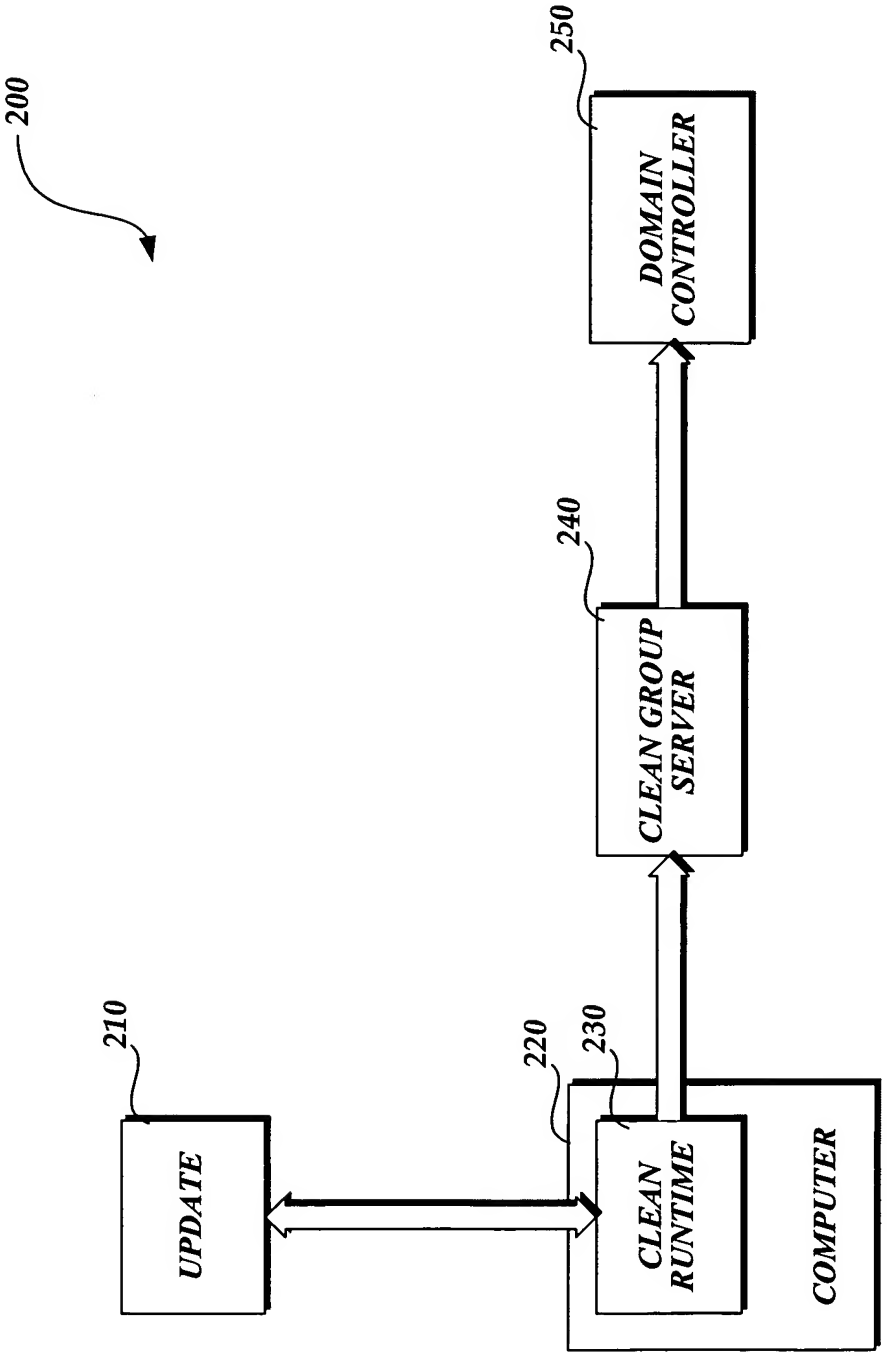
200
250
DOMAIN CONTROLLER
240
CLEAN GROUP SERVER
210
220
230
UPDATE
CLEAN RUNTIME
COMPUTER

Fig.2.

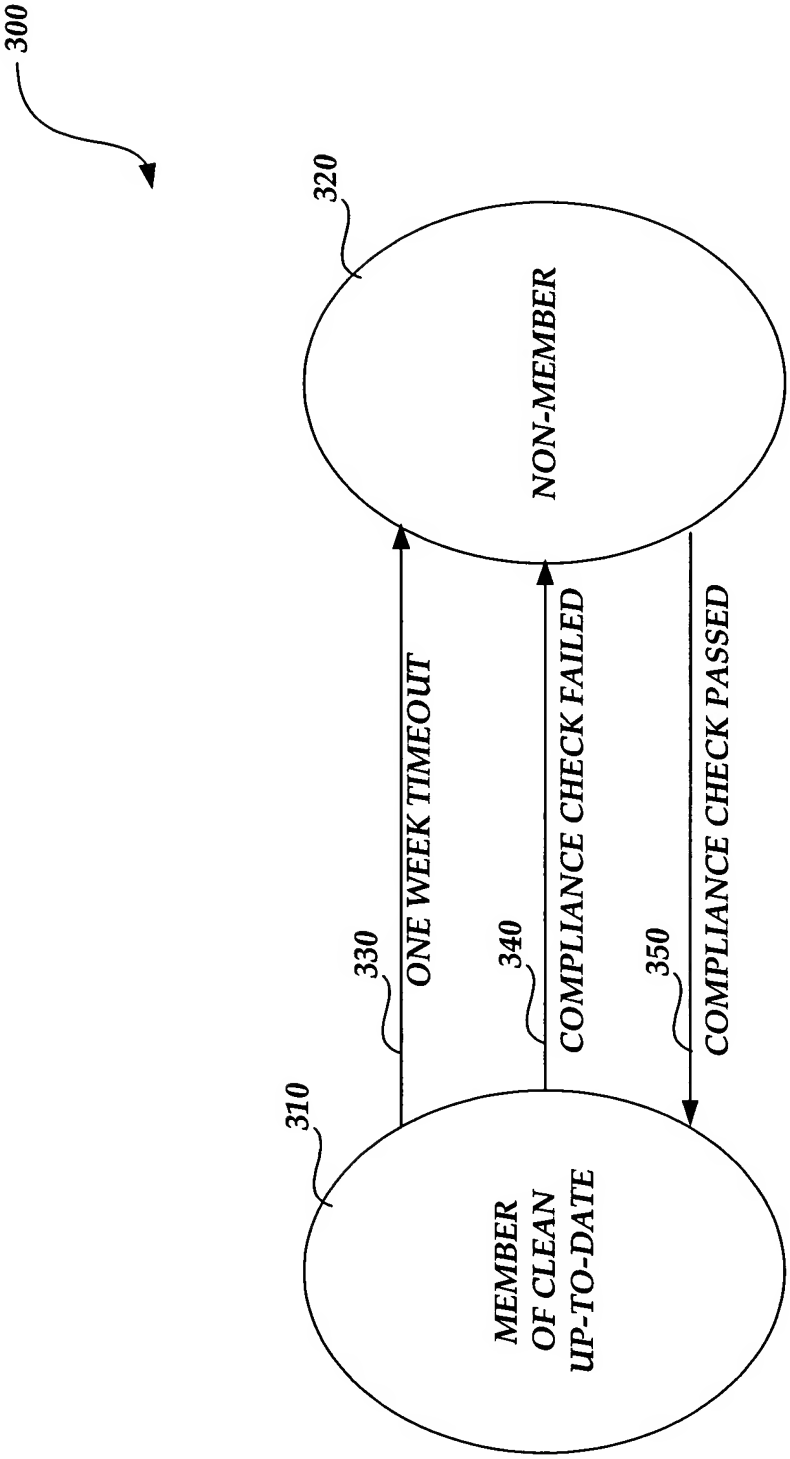
300
320
NON-MEMBER
330
ONE WEEK TIMEOUT
340
COMPLIANCE CHECK FAILED
350
COMPLIANCE CHECK PASSED
310
MEMBER OF CLEAN UP-TO-DATE

Fig.3.

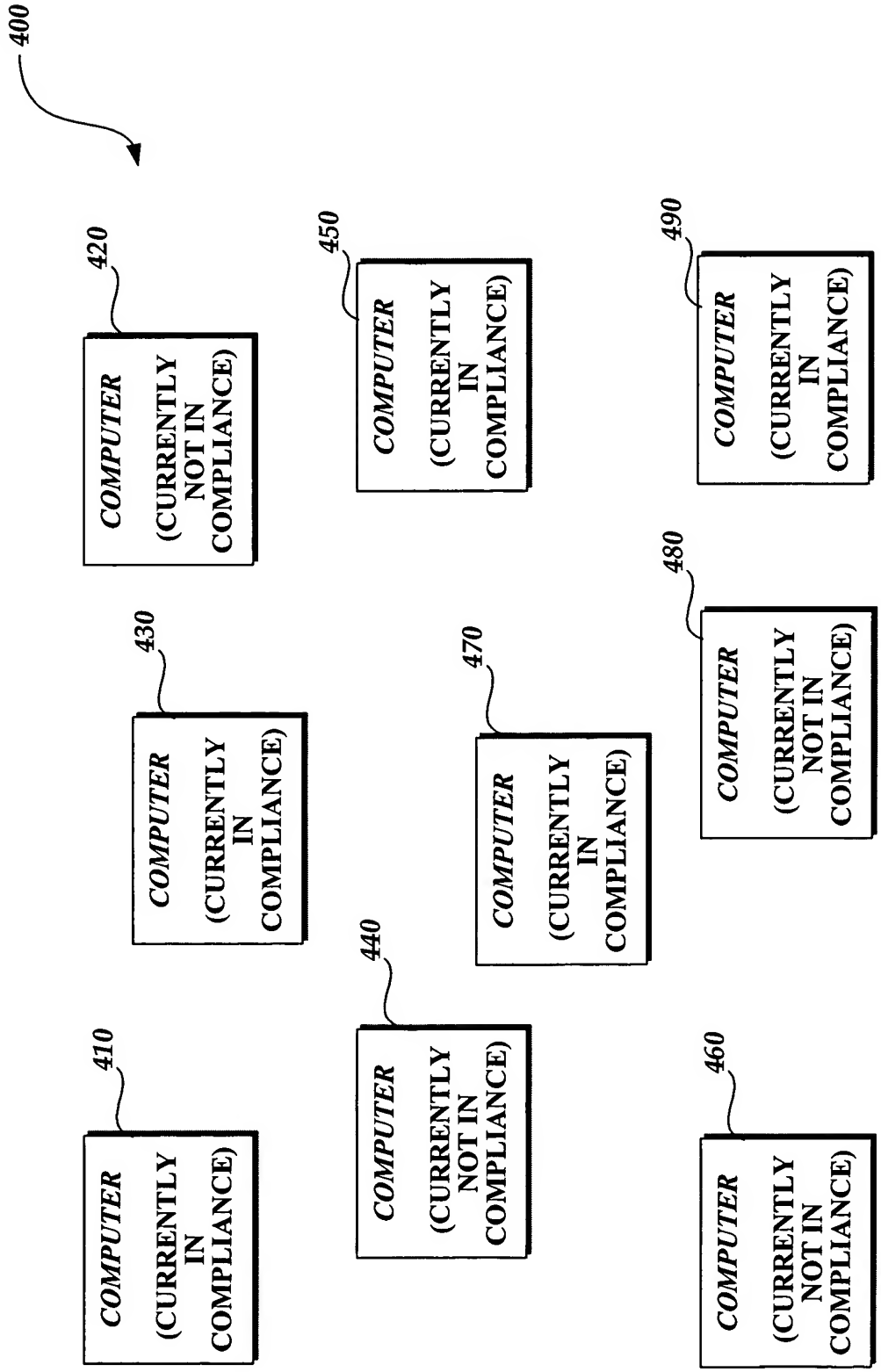
400
420
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
450
COMPUTER (CURRENTLY IN COMPLIANCE)
490
COMPUTER (CURRENTLY IN COMPLIANCE)
430
COMPUTER (CURRENTLY IN COMPLIANCE)
470
COMPUTER (CURRENTLY IN COMPLIANCE)
480
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
410
COMPUTER (CURRENTLY IN COMPLIANCE)
440
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
460
COMPUTER (CURRENTLY NOT IN COMPLIANCE)

Fig. 4A.

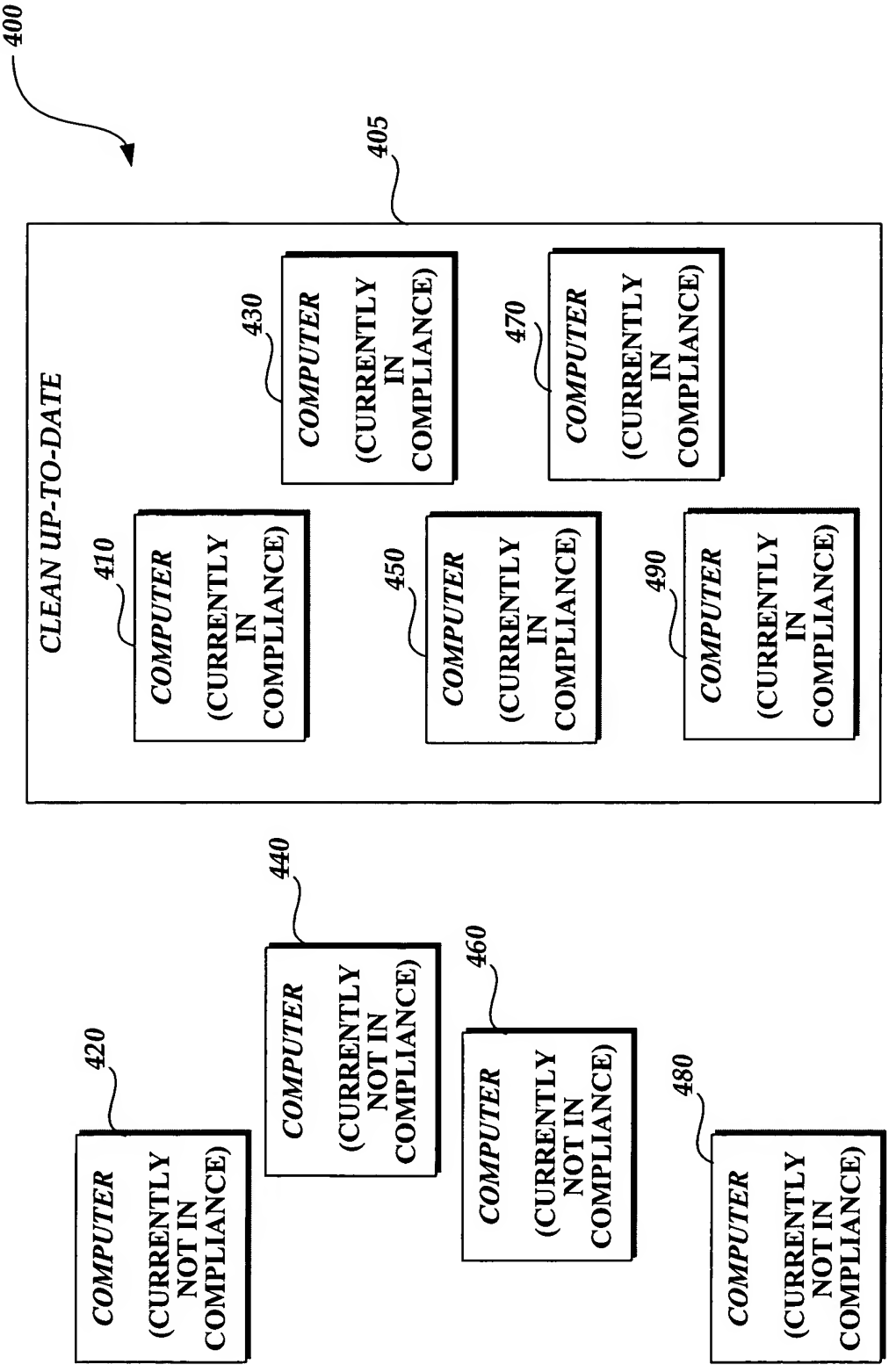
400
405
CLEAN UP-TO-DATE
410
COMPUTER (CURRENTLY IN COMPLIANCE)
430
COMPUTER (CURRENTLY IN COMPLIANCE)
450
COMPUTER (CURRENTLY IN COMPLIANCE)
470
COMPUTER (CURRENTLY IN COMPLIANCE)
490
COMPUTER (CURRENTLY IN COMPLIANCE)
420
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
440
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
460
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
480
COMPUTER (CURRENTLY NOT IN COMPLIANCE)

Fig.4B.

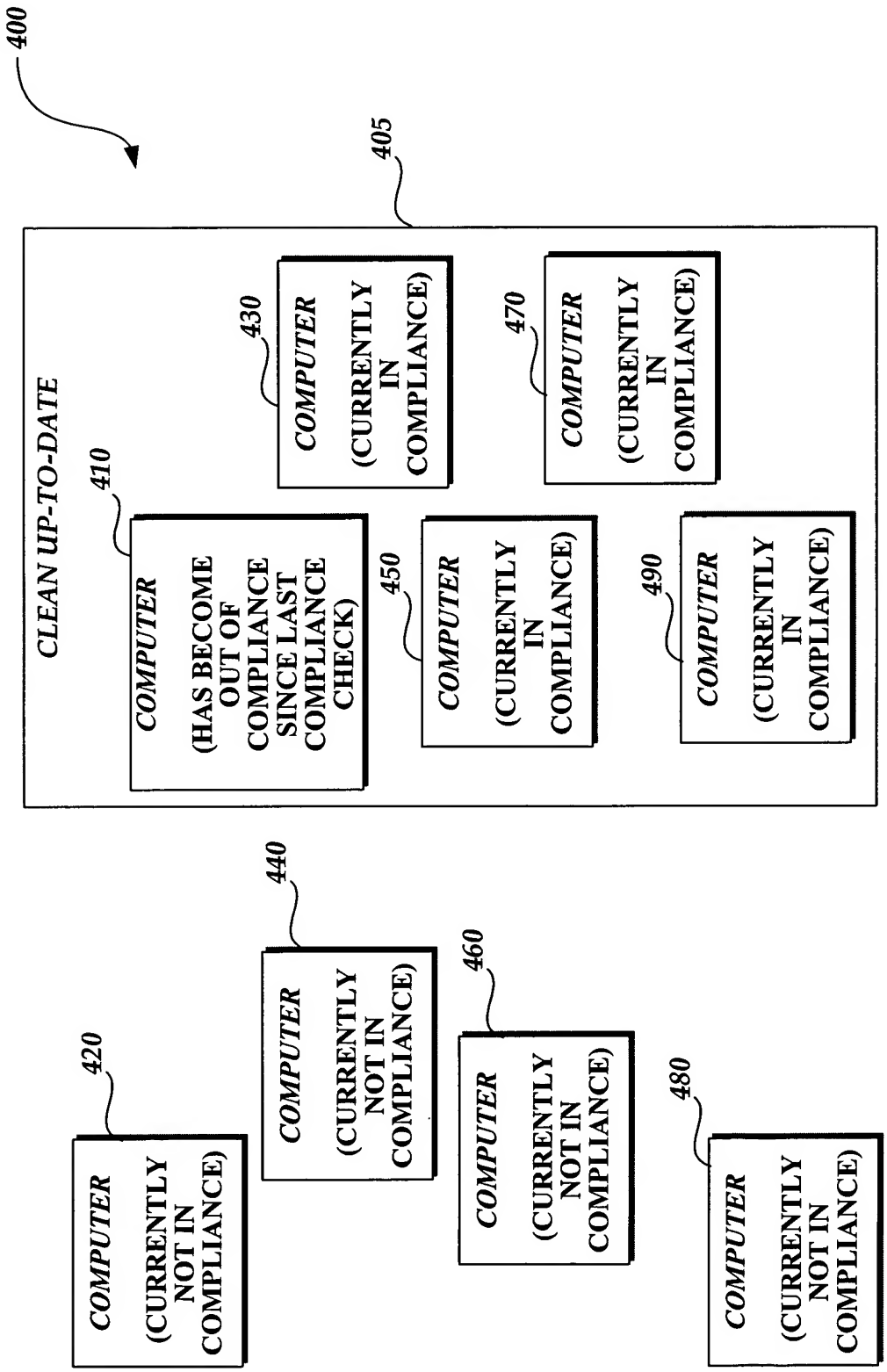
400
405
CLEAN UP-TO-DATE
410
COMPUTER (HAS BECOME OUT OF COMPLIANCE SINCE LAST COMPLIANCE CHECK)
430
COMPUTER (CURRENTLY IN COMPLIANCE)
450
COMPUTER (CURRENTLY IN COMPLIANCE)
470
COMPUTER (CURRENTLY IN COMPLIANCE)
490
COMPUTER (CURRENTLY IN COMPLIANCE)
420
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
440
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
460
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
480
COMPUTER (CURRENTLY NOT IN COMPLIANCE)

Fig.4C.

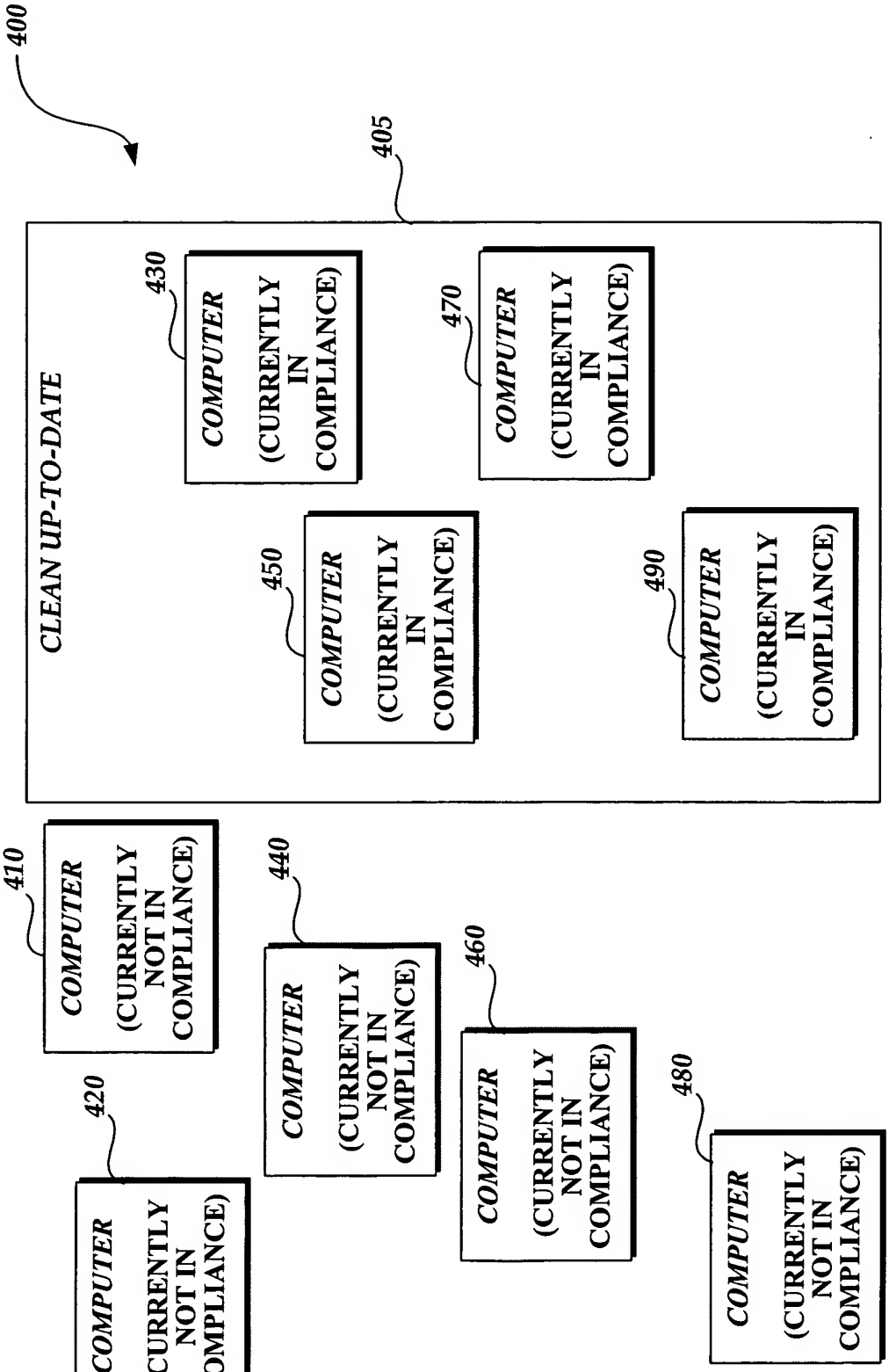
400
405
CLEAN UP-TO-DATE
430
COMPUTER (CURRENTLY IN COMPLIANCE)
470
COMPUTER (CURRENTLY IN COMPLIANCE)
450
COMPUTER (CURRENTLY IN COMPLIANCE)
490
COMPUTER (CURRENTLY IN COMPLIANCE)
410
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
440
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
460
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
480
COMPUTER (CURRENTLY NOT IN COMPLIANCE)
420
COMPUTER (CURRENTLY NOT IN COMPLIANCE)

Fig.4D.

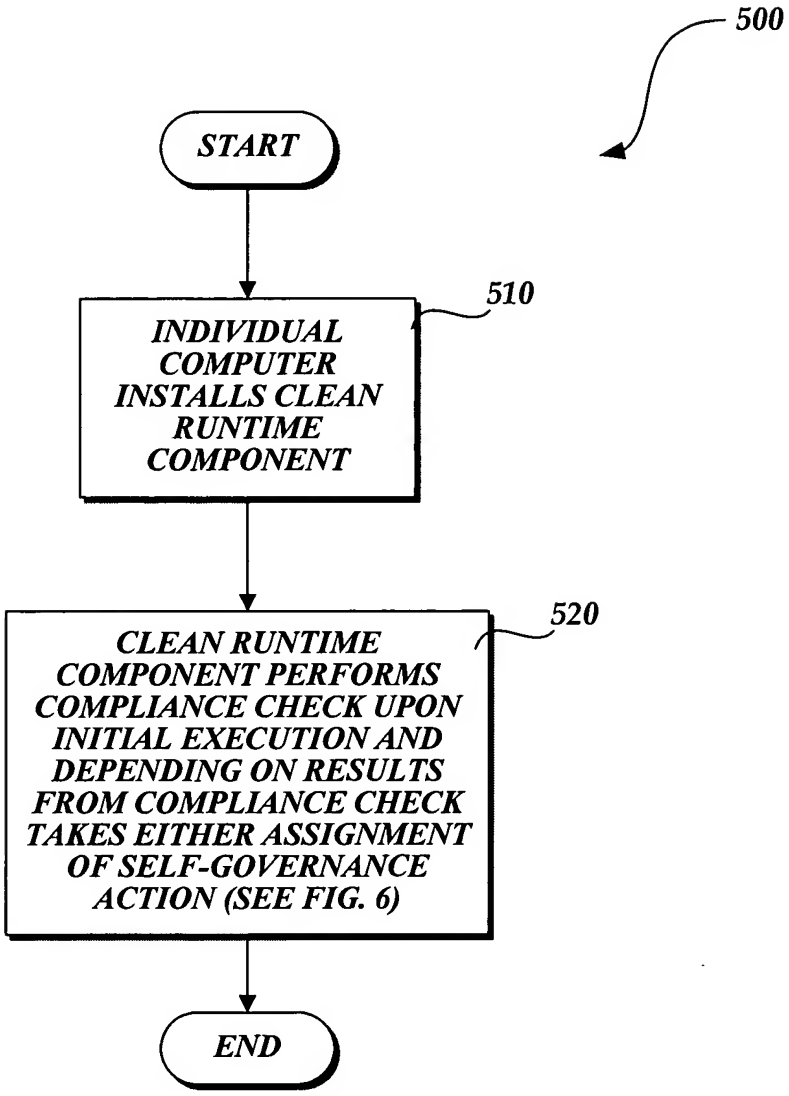
500
START
510
INDIVIDUAL COMPUTER INSTALLS CLEAN RUNTIME COMPONENT
520
CLEAN RUNTIME COMPONENT PERFORMS COMPLIANCE CHECK UPON INITIAL EXECUTION AND DEPENDING ON RESULTS FROM COMPLIANCE CHECK TAKES EITHER ASSIGNMENT OF SELF-GOVERNANCE ACTION (SEE FIG. 6)
END

Fig. 5.

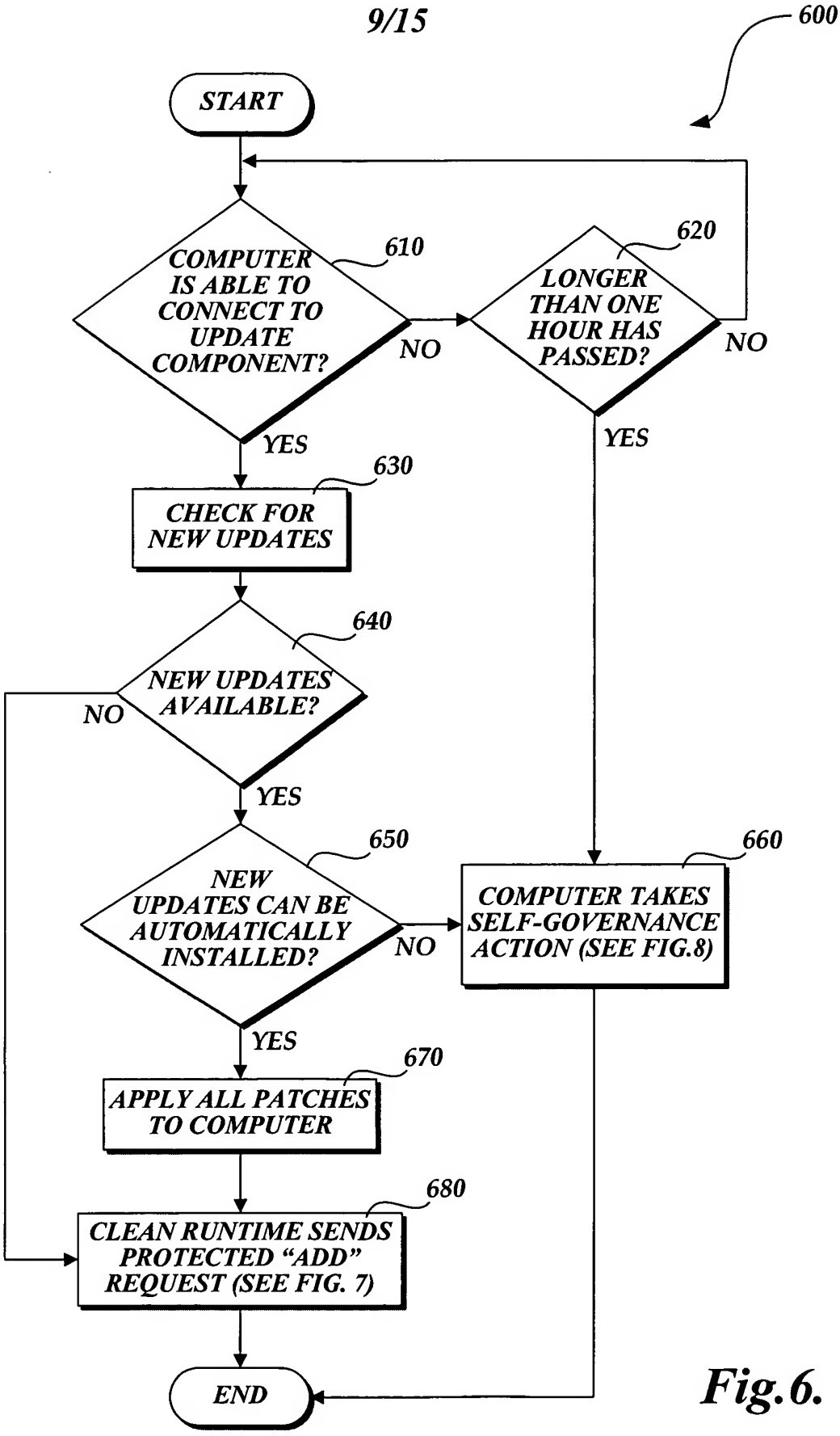
600
START
COMPUTER IS ABLE TO CONNECT TO UPDATE COMPONENT?
610
NO
YES
LONGER THAN ONE HOUR HAS PASSED?
620
NO
YES
CHECK FOR NEW UPDATES
630
NEW UPDATES AVAILABLE?
640
NO
YES
NEW UPDATES CAN BE AUTOMATICALLY INSTALLED?
650
NO
YES
COMPUTER TAKES SELF-GOVERNANCE ACTION (SEE FIG.8)
660
APPLY ALL PATCHES TO COMPUTER
670
CLEAN RUNTIME SENDS PROTECTED "ADD" REQUEST (SEE FIG. 7)
680
END

Fig. 6.

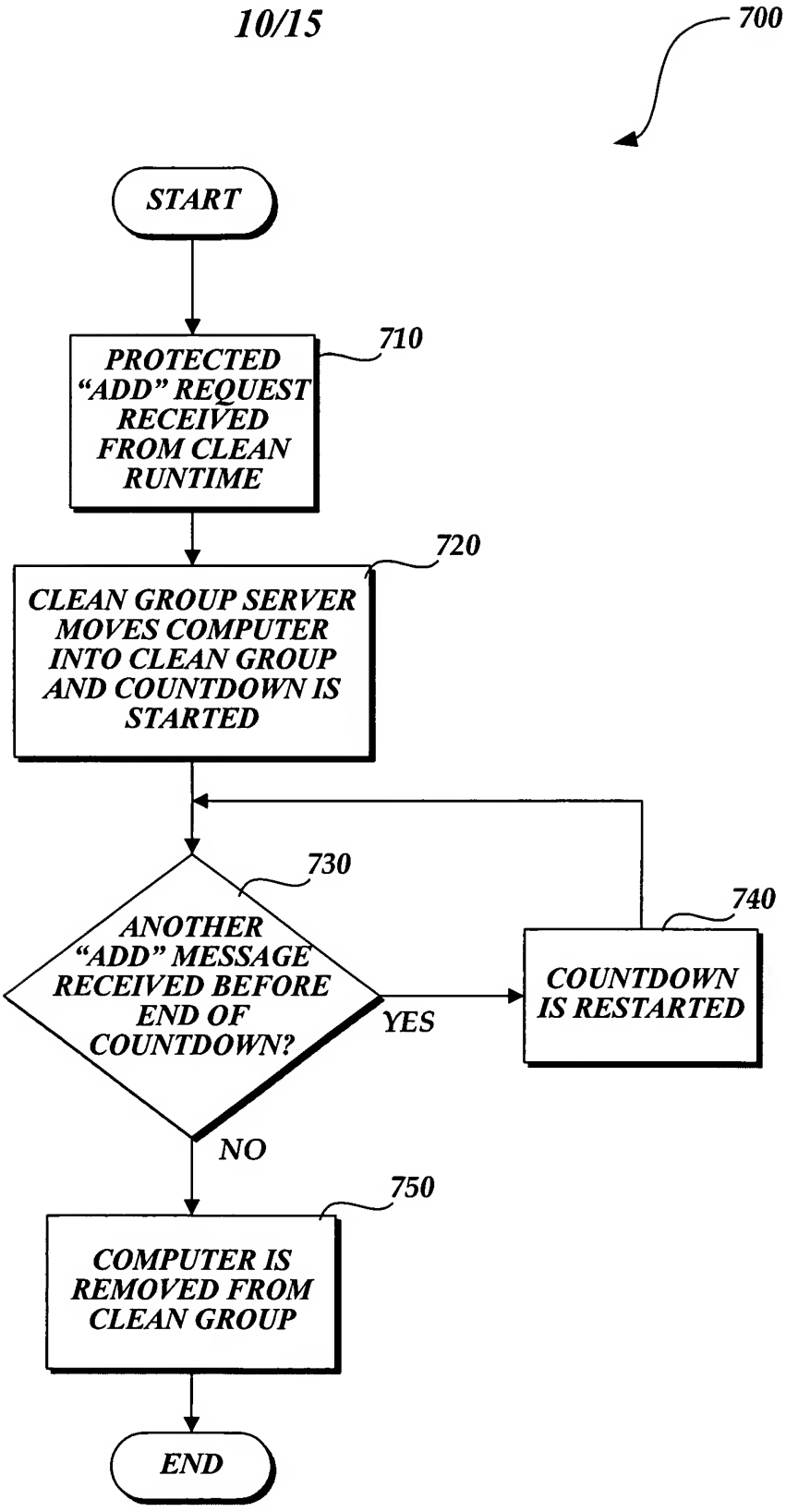
700
START
710
PROTECTED "ADD" REQUEST RECEIVED FROM CLEAN RUNTIME
720
CLEAN GROUP SERVER MOVES COMPUTER INTO CLEAN GROUP AND COUNTDOWN IS STARTED
730
ANOTHER "ADD" MESSAGE RECEIVED BEFORE END OF COUNTDOWN?
YES
740
COUNTDOWN IS RESTARTED
NO
750
COMPUTER IS REMOVED FROM CLEAN GROUP
END

Fig. 7.

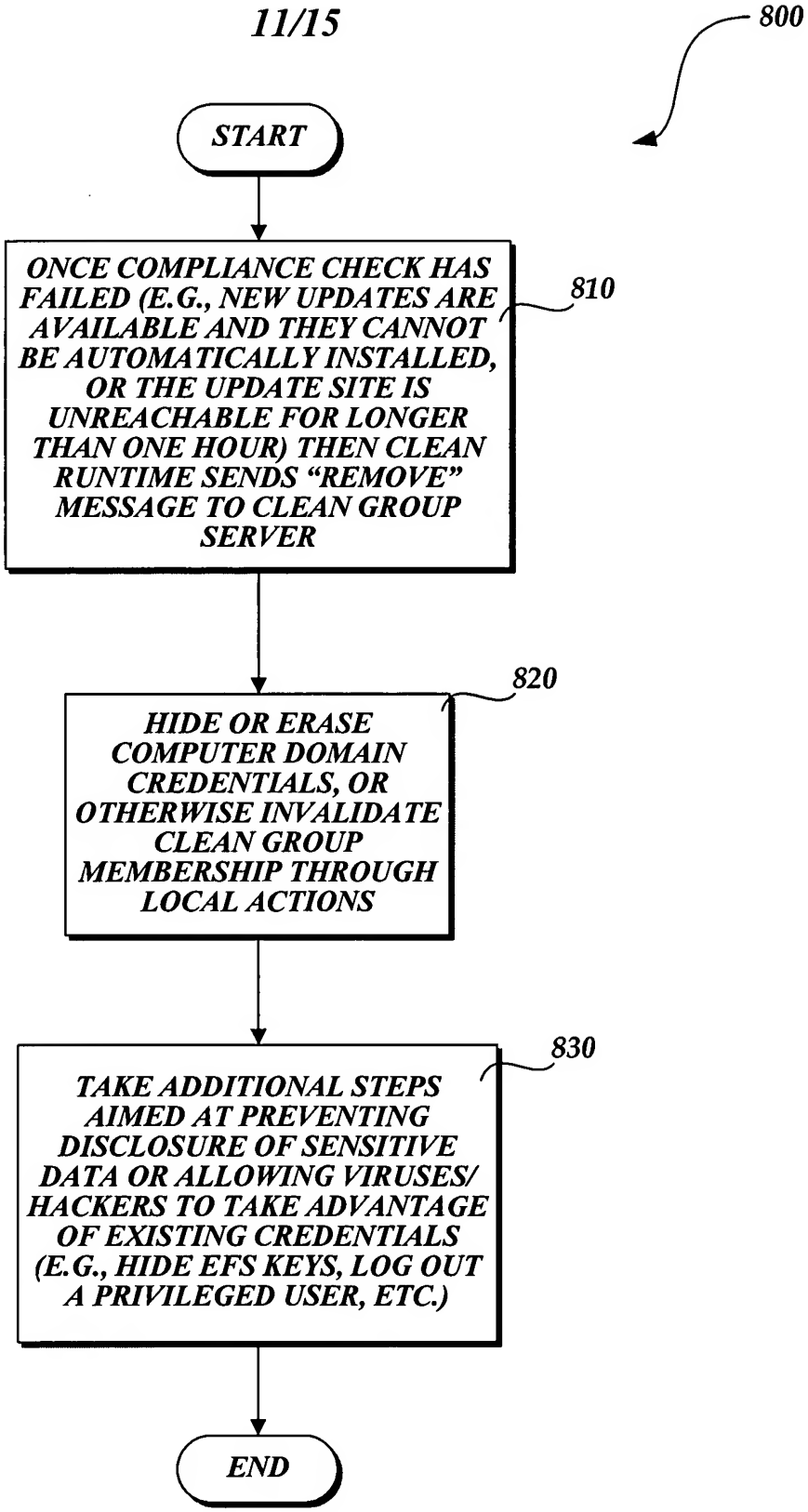
800
START
ONCE COMPLIANCE CHECK HAS FAILED (E.G., NEW UPDATES ARE AVAILABLE AND THEY CANNOT BE AUTOMATICALLY INSTALLED, OR THE UPDATE SITE IS UNREACHABLE FOR LONGER THAN ONE HOUR) THEN CLEAN RUNTIME SENDS "REMOVE" MESSAGE TO CLEAN GROUP SERVER
810
HIDE OR ERASE COMPUTER DOMAIN CREDENTIALS, OR OTHERWISE INVALIDATE CLEAN GROUP MEMBERSHIP THROUGH LOCAL ACTIONS
820
TAKE ADDITIONAL STEPS AIMED AT PREVENTING DISCLOSURE OF SENSITIVE DATA OR ALLOWING VIRUSES/ HACKERS TO TAKE ADVANTAGE OF EXISTING CREDENTIALS (E.G., HIDE EFS KEYS, LOG OUT A PRIVILEGED USER, ETC.)
830
END

Fig. 8.

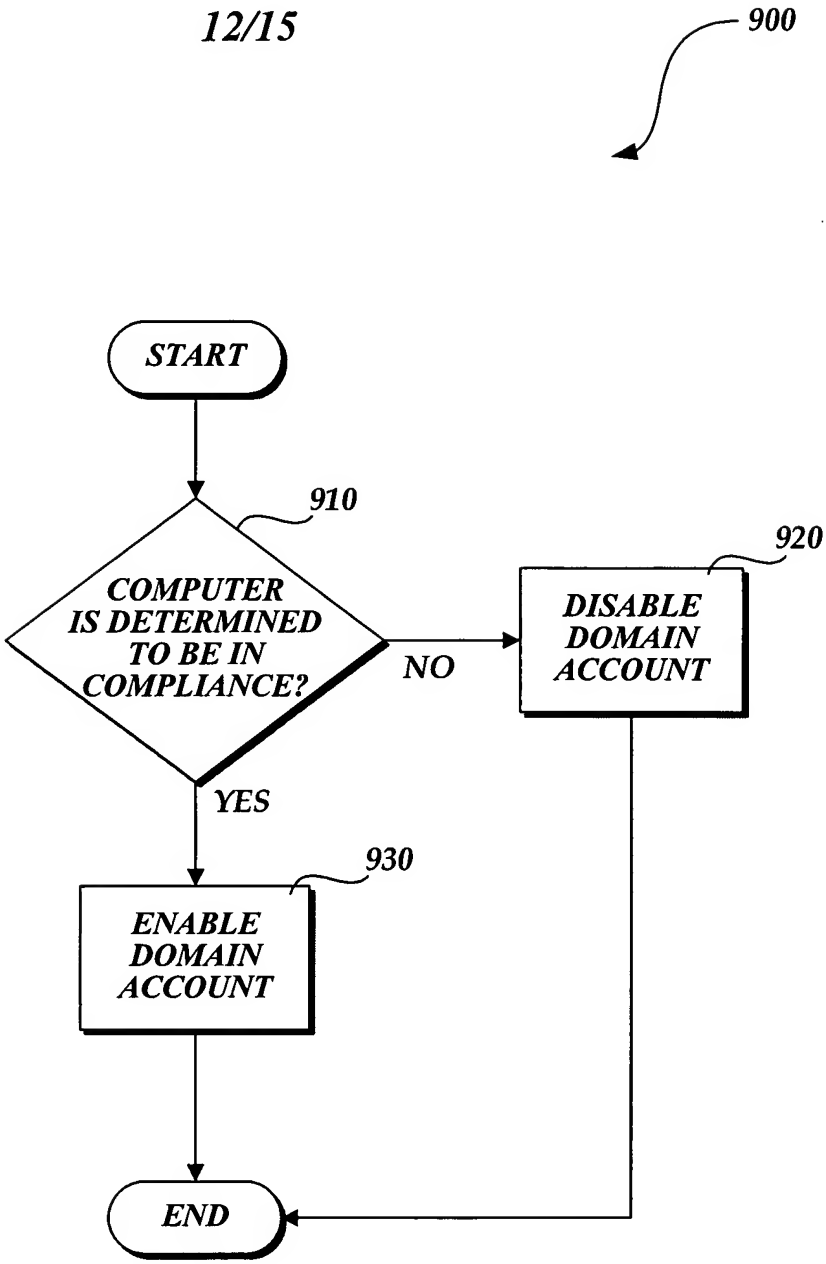
900
START
910
COMPUTER IS DETERMINED TO BE IN COMPLIANCE?
NO
920
DISABLE DOMAIN ACCOUNT
YES
930
ENABLE DOMAIN ACCOUNT
END

Fig. 9.

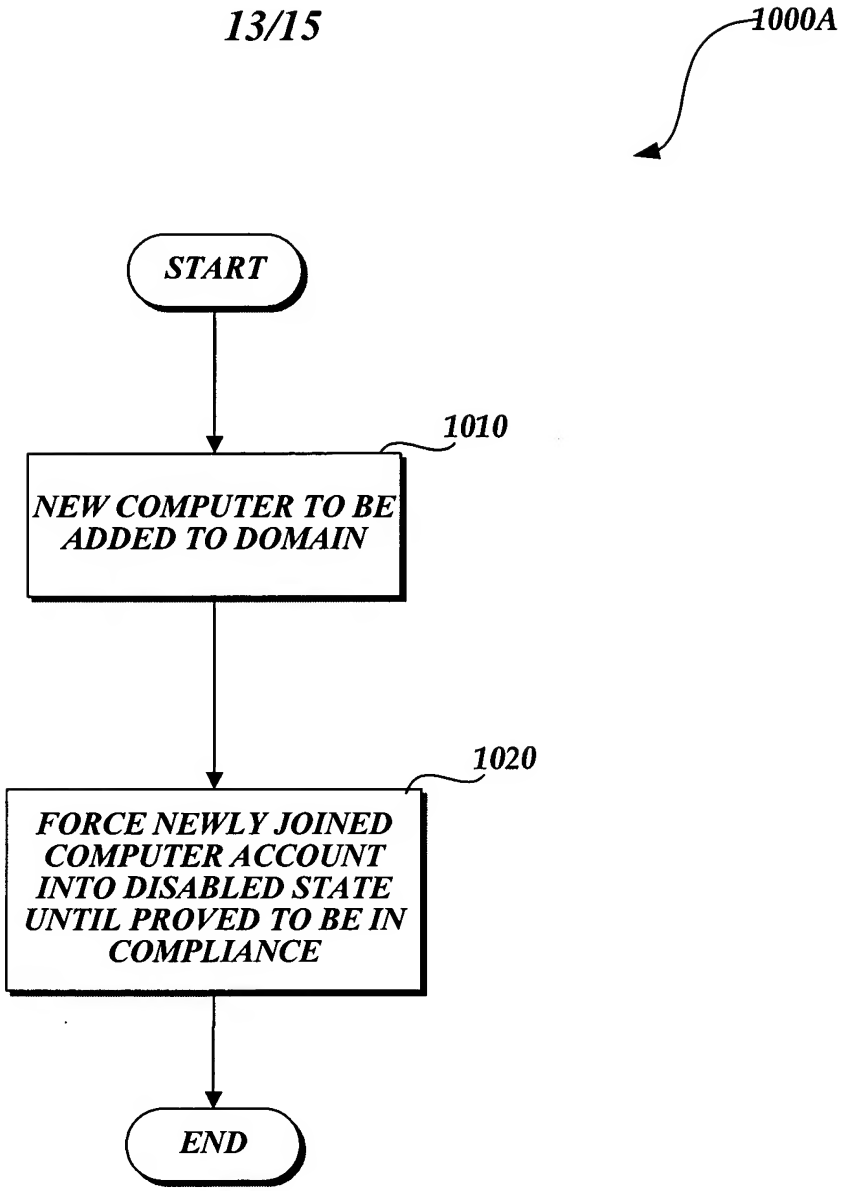
1000A
START
1010
NEW COMPUTER TO BE ADDED TO DOMAIN
1020
FORCE NEWLY JOINED COMPUTER ACCOUNT INTO DISABLED STATE UNTIL PROVED TO BE IN COMPLIANCE
END

Fig.10A.

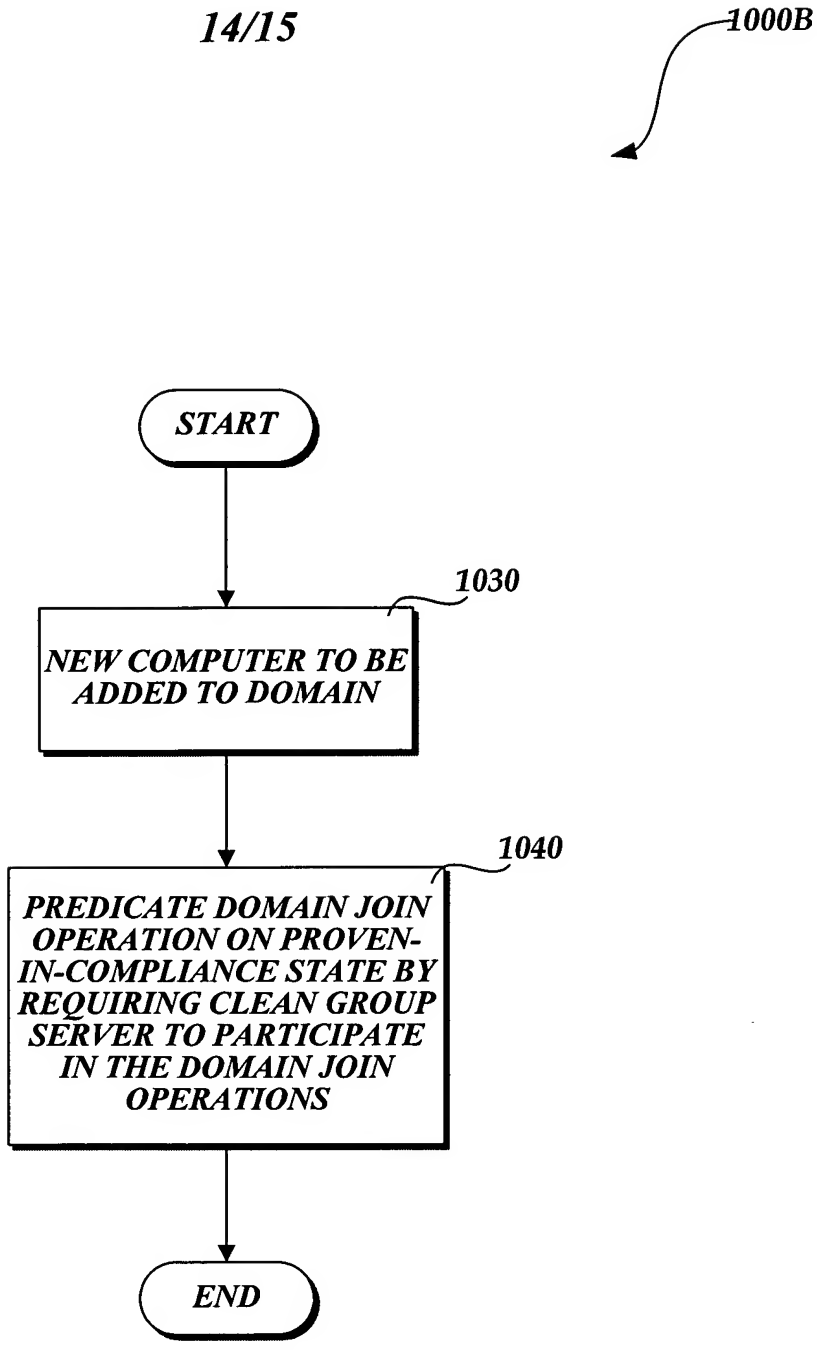
1000B
START
1030
NEW COMPUTER TO BE ADDED TO DOMAIN
1040
PREDICATE DOMAIN JOIN OPERATION ON PROVEN-IN-COMPLIANCE STATE BY REQUIRING CLEAN GROUP SERVER TO PARTICIPATE IN THE DOMAIN JOIN OPERATIONS
END

Fig.10B.

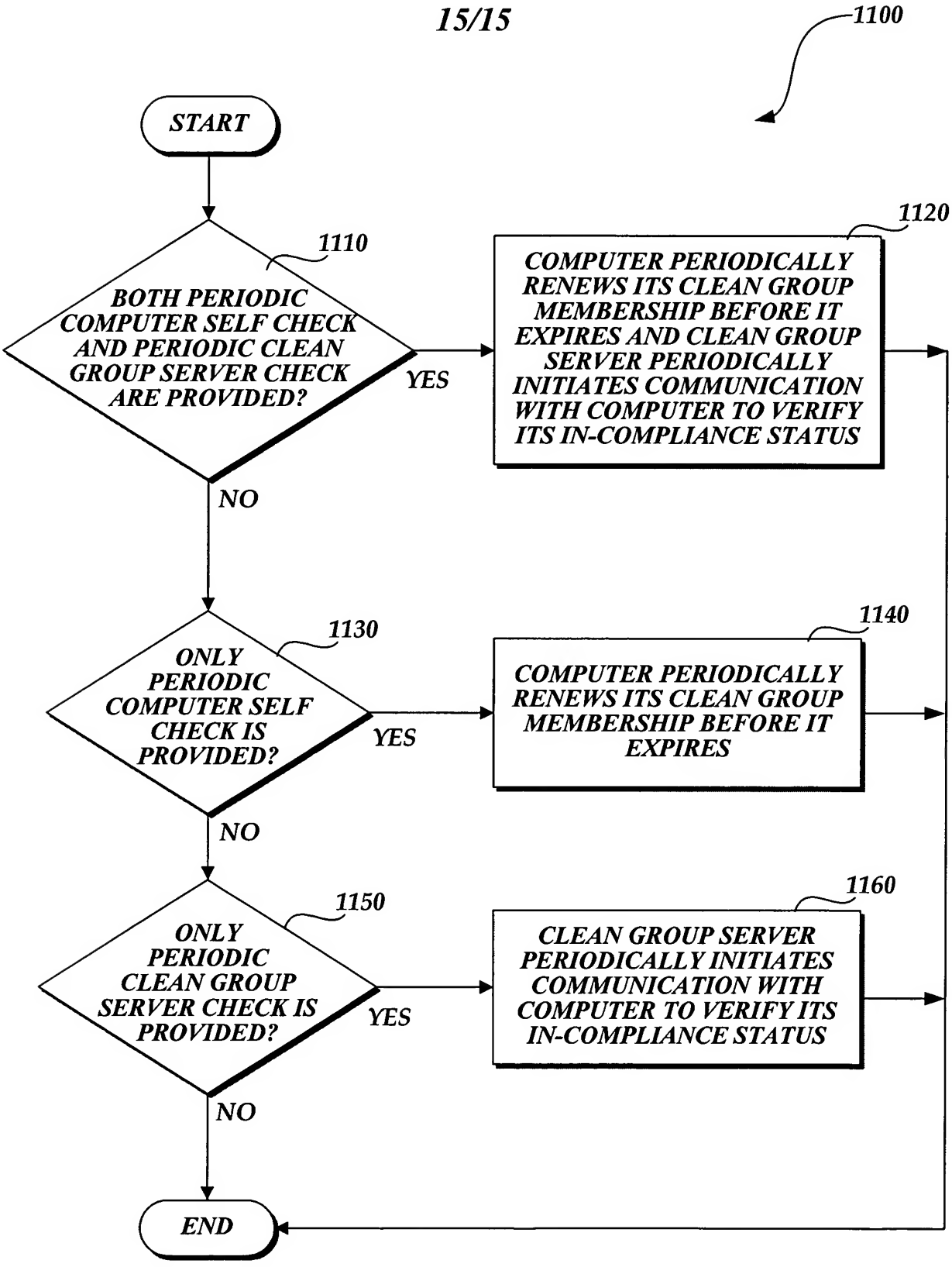
1100
START
1110
BOTH PERIODIC COMPUTER SELF CHECK AND PERIODIC CLEAN GROUP SERVER CHECK ARE PROVIDED?
YES
1120
COMPUTER PERIODICALLY RENEWS ITS CLEAN GROUP MEMBERSHIP BEFORE IT EXPIRES AND CLEAN GROUP SERVER PERIODICALLY INITIATES COMMUNICATION WITH COMPUTER TO VERIFY ITS IN-COMPLIANCE STATUS
NO
1130
ONLY PERIODIC COMPUTER SELF CHECK IS PROVIDED?
YES
1140
COMPUTER PERIODICALLY RENEWS ITS CLEAN GROUP MEMBERSHIP BEFORE IT EXPIRES
NO
1150
ONLY PERIODIC CLEAN GROUP SERVER CHECK IS PROVIDED?
YES
1160
CLEAN GROUP SERVER PERIODICALLY INITIATES COMMUNICATION WITH COMPUTER TO VERIFY ITS IN-COMPLIANCE STATUS
NO
END

Fig.11.